NISTIR 4387

U.S. DEPARTMENT OF JUSTICE SIMPLIFIED RISK ANALYSIS GUIDELINES

NEW NIST PUBLICATION

December 1990

Edward Roback
NIST Coordinator

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, MD 20899

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
John W. Lyons, Director

NIST

NISTIR 4387

U.S. DEPARTMENT OF JUSTICE SIMPLIFIED RISK ANALYSIS GUIDELINES

Edward Roback
NIST Coordinator

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, MD 20899

August 1990

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
John W. Lyons, Director

Preface

This National Institute of Standards and Technology Interagency Report (NISTIR) presents the Simplified Risk Analysis Guidelines developed by the U.S. Department of Justice, Justice Management Division, Security and Emergency Planning Staff, ADP/Telecommunications Group.

The National Institute of Standards and Technology (NIST) makes no claim or endorsement of this risk analysis methodology. However, as this material may be of use to other organizations, the report is being reprinted by NIST to make it publicly available and to provide for broad dissemination of this federally sponsored work. This publication is part of a continuing effort to assist federal agencies in accordance with NIST's mandate under the Computer Security Act of 1987.

NIST expresses its appreciation to the U.S. Department of Justice for their permission to publish this report.

Questions regarding this publication should be addressed to the Associate Director for Computer Security, National Computer Systems Laboratory, Building 225, Room B154, National Institute of Standards and Technology, Gaithersburg, MD, 20899.

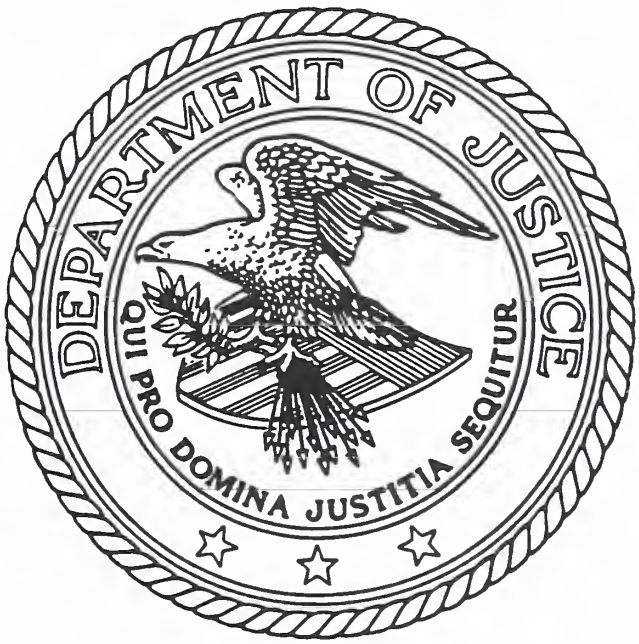
Additional copies of this publication may be purchased through the National Technical Information Service, Springfield, VA, 22161, telephone: (703) 487-4650.

U.S. Department of Justice
Justice Management Division

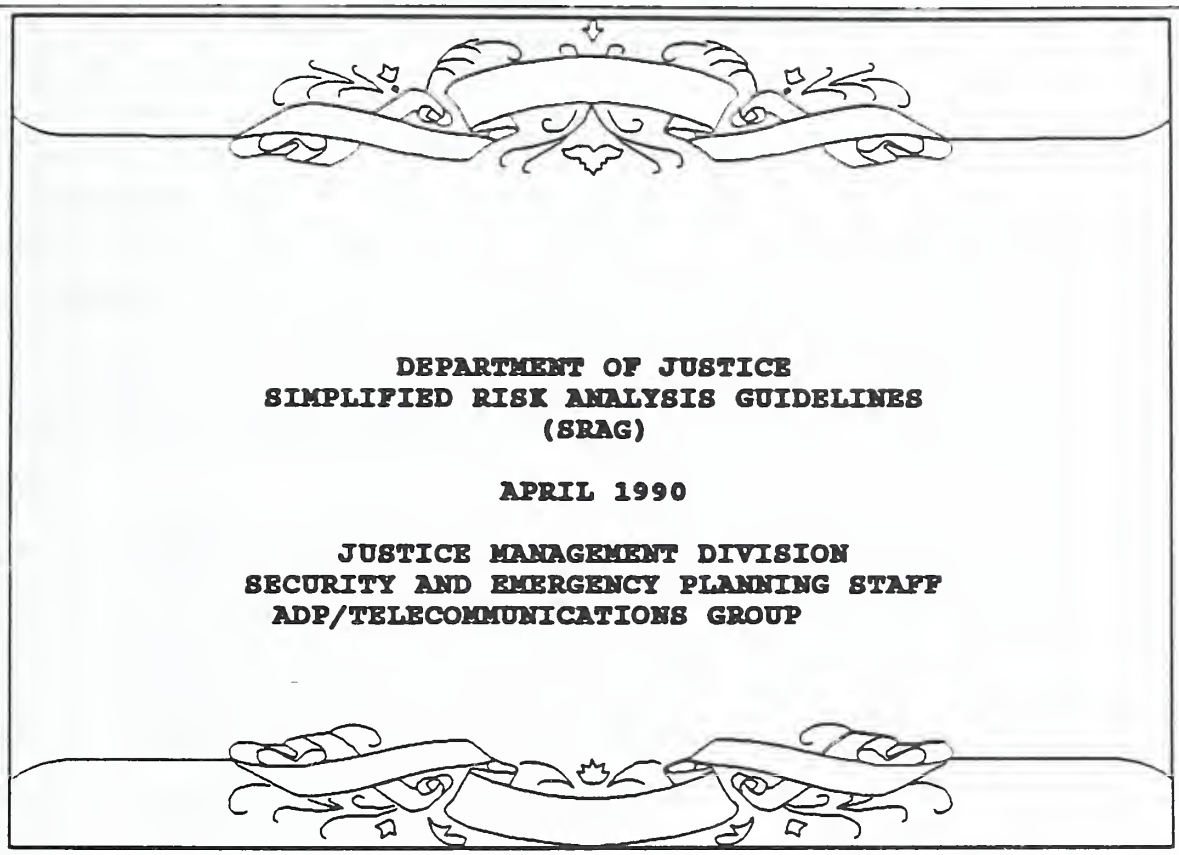
Security Guidelines

DEPARTMENT OF JUSTICE
SIMPLIFIED RISK ANALYSIS
GUIDELINES
(SRAG)

APRIL 1990



Prepared by:
Security and Emergency Planning Staff



DEPARTMENT OF JUSTICE
SIMPLIFIED RISK ANALYSIS GUIDELINES
(SRAG)

APRIL 1990

JUSTICE MANAGEMENT DIVISION
SECURITY AND EMERGENCY PLANNING STAFF
ADP/TELECOMMUNICATIONS GROUP

DEPARTMENT OF JUSTICE
SIMPLIFIED RISK ANALYSIS GUIDELINES
APRIL 1990

TABLE OF CONTENTS

FIGURES

TABLES

WORK FORMS

DEPARTMENT OF JUSTICE

SIMPLIFIED RISK ANALYSIS GUIDELINES

1. INTRODUCTION.

a. A risk analysis may be defined as an analysis of the threats to and vulnerabilities of a system, expected losses, and selection of countermeasures to reduce the losses to an acceptable level. The requirement for Federal agencies to conduct a risk analysis of an Automated Data Processing (ADP) facility has been in effect since the issuance of the Office of Management and Budget (OMB) Circular A-71, Transmittal Memorandum No. 1 in 1978. The Department of Justice (DOJ) issued Order DOJ 2640.2B and its earlier canceled versions which established the requirement for a risk analysis of DOJ ADP facilities beginning in 1977. The DOJ also issued a detailed risk analysis guidance document for use by DOJ ADP facilities in 1977. A number of Federal agencies, contractors, and university professors have developed risk analysis methodologies, some of which have been automated. Due to the complexity of the risk analysis process, the methodologies generally require considerable time to become knowledgeable of its correct usage and to complete the risk analysis.

b. A risk analysis does not enhance security by itself but provides cost effective security recommendations for management consideration. Therefore, there is a need to simplify the risk analysis process to the extent possible, which is the intent of the Simplified Risk Analysis Guidelines (SRAG) contained herein. The SRAG expedites the risk analysis process for the system under evaluation by initially determining if minimum security requirements applicable to the DOJ are met, which eliminates a number of threats and losses from evaluation. Although the SRAG simplifies the risk analysis process, SRAG users should be aware that significant effort by knowledgeable personnel may be required to complete a risk analysis. The SRAG is based on Automated Information System (AIS) security policies, regulations, circulars, and guidelines applicable to the DOJ as well as a review of a number of risk analysis methodologies developed by Government agencies and contractors.

c. After evaluating compliance with the minimum security requirements, additional threats and vulnerabilities not affected by the minimum security requirements are assessed to determine if further analysis is needed. The SRAG or a risk analysis methodology selected by the user can be used for this portion of the risk analysis process. Due to the increasing use of AISs other than mainframes, the SRAG also includes sections on microcomputers/Personal Computers (PCs) and application systems. The sections applicable to mainframes are also applicable to minicomputers and other remotely accessed AISs, including networks of PCs.

2. BACKGROUND.

a. Various risk analysis methodologies have been developed by contractors and agencies since the issuance of the risk analysis guidelines by the National Bureau of Standards (NBS) of Federal Information Processing Standard (FIPS) Publication (PUB) 31, "Guidelines for ADP Physical Security and Risk Management" in 1974, and FIPS PUB 65, "Guideline for ADP Risk Assessment" in 1979. The NBS publications advocated the use of quantitative techniques assigning dollar values to system losses and estimating the annual probability of threats occurring to cause these losses. Similarly, dollar figures are assigned to the cost of security countermeasures and to the reduction in expected annual losses to determine the cost effectiveness of the security measure.

b. Although the National Institute of Standards and Technology (name of NBS since 1988) has not issued any risk analysis publications recently, they are presently considering methodologies using qualitative analysis in part or as a primary method of risk analysis. The methodologies that have been developed are primarily for the mainframe environment despite the increase in usage of PCs and networks and include the use of both quantitative and qualitative techniques. As stated previously, the SRAG does not require or preclude the use of any specific methodology and may be used to conduct a risk analysis of an AIS in many cases without additional risk analysis guidance.

3. DEFINITIONS.

a. Accreditation - Accreditation is the official management authorization to operate an AIS or network in a particular security mode with a proscribed set of administrative, environmental, and technical security safeguards in a given operational environment.

b. Automated Information System (AIS) - An AIS is an assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information. An AIS will typically consist of ADP system hardware, operating system and application software, associated peripheral devices, and associated data communications equipment. An AIS includes PCs, work stations, and office automation systems.

c. Network - A network comprises communications media and all attached components whose responsibility is the transfer of information among a collection of AISs or work stations. Network components include packet switches, front-end computers, network controllers, and technical control devices.

d. Sensitive Application Systems - Systems that process sensitive data or require protection due to the risk and magnitude of loss or harm that could result from improper operation or deliberate manipulation of the application.

4. DESCRIPTION OF SRAG APPROACH.

a. The SRAG approach divides systems requiring risk analyses into three categories: PCs; mainframes, minicomputers, and other remotely accessed AISs; and application systems. Each of these categories is further divided depending on whether nonsensitive, sensitive, or classified information is processed, or whether an application is nonsensitive or sensitive as defined in OMB Circular A-130, Appendix III.

b. The SRAG includes seven steps that are required to conduct the risk analysis and to document the results. The first two steps are used to provide a description of the AIS, its security concerns, and the security measures in place. In Step 3, the AIS environment is evaluated to determine if minimum security requirements are met. The minimum security requirements are listed for processing nonsensitive, sensitive, and classified information on PCs. It should be noted that the minimum security requirements for processing sensitive information also include the requirements for processing nonsensitive; processing classified information requires meeting the minimum security requirements for classified, sensitive, and nonsensitive information. The minimum security requirements for mainframes, minicomputers, and other remotely accessed AISs are presented in a similar hierarchical structure. Sensitive applications must meet the minimum requirements listed for sensitive and nonsensitive applications.

c. The remaining steps are used for the following: To determine from an analysis of threats and losses whether additional security measures need to be considered; to select security measures to comply with the minimum requirements that are not effectively met and to reduce other losses; to provide for cost effective recommendations of security measures; to present the recommendations for a decision by management whether to implement the recommendations or accept the risk; and to document the results. The seven SRAG steps are discussed briefly below, followed by Section 12, which provides instructions for using the SRAG and includes flow charts and other information to assist SRAG users. The last portion of the SRAG is the Appendix, which includes detailed information required to conduct a risk analysis, and a number of tables and work forms for use in conducting and documenting the risk analysis.

5. STEP 1. <u>SYSTEM DESCRIPTION</u>.

a. The purpose of Step 1 is to provide a system description of the AIS including the system hardware, software, and personnel, and a general description of the applications and data processed by the AIS. If a risk analysis of an application system is being conducted, a description of the purpose and use of the system is required. Estimates of the cost of the system components should also be included.

b. The detailed information required is listed in Table 1 of the Appendix and includes administrative information such as the name and location of the AIS and the names and phone numbers of AIS security personnel. The purpose of the AIS and the component functions it supports should be noted.

c. The system configuration includes a detailed description of the physical location, system configuration diagram, connections, number of users, system and application personnel, and the application systems. A brief description of the purpose of the applications, their method of data input, and the users of the system data should also be included. Cost information required includes the cost of replacing system hardware and software, and the cost of replacing data. The cost information is useful in determining if security countermeasures to reduce the vulnerabilities and potential losses are cost effective. The information obtained during this step is important in evaluating the potential vulnerabilities of the system and the need for additional security measures. It is only through a review of all system components, the applications processed, and the flow of information that an effective analysis of the potential system vulnerabilities can be obtained.

6. STEP 2. AIS SECURITY INFORMATION.

a. In Step 2 of the risk analysis, security related information for the AIS or application is obtained and documented. The system security measures in effect are identified and documented with a brief evaluation of their effectiveness. Security measures are required even if nonsensitive information is processed to protect the equipment and integrity of the data. However, central to the determination of the need for additional security measures is the type of information processed, whether classified (National Security Information), sensitive (Limited Official Use) or nonsensitive information, and the threats to this information. This information is important in determining which minimum security requirements are applicable. The Appendix contains a list of the factors that should be carefully considered during this step, including a list of security measures (Table 2) and application system data sensitivity and criticality considerations (Table 3 and Work Form 5).

b. This step also requires an accurate documentation of the security policies, procedures, and countermeasures currently in effect for the AIS. The security measures in place should include administrative procedures, software and hardware security controls, physical security access controls, personnel security controls, and a security awareness program as listed in Table 2. The current security control environment is important due to its impact on the evaluation of the need for additional security measures.

c. The person conducting the risk analysis should also obtain information on the impact of data disclosure, modification, destruction, and disruption of processing on the component's ability to meet mission objectives. The information obtained during Step 2 should be documented using Work Forms 2, 3, 4, and 5. Additional information required by this step includes the number and geographical disparity of AIS users, the frequency of use of the system, and the method of accessing the system.

7. STEP 3. MINIMUM SECURITY REQUIREMENTS.

a. The minimum security requirements for PCs, mainframes, minicomputers, and other remotely accessed AISs, and application systems are listed in Sections 3.1, 3.2, and 3.3 of the Appendix. The requirements of each of these sections are divided into requirements for nonsensitive, sensitive, and classified processing for Sections 3.1 and 3.2, and nonsensitive and sensitive applications for Section 3.3. The minimum security requirements are hierarchical in structure, so that requirements for processing lower sensitivity levels also are applicable to all higher sensitivity levels.

b. This step requires a review of the minimum security requirements as listed in the Appendix for the AIS or application under evaluation. The review also requires an evaluation of the effectiveness of the in-place security measures in meeting the security requirement. The person conducting the risk analysis must identify all security measures implemented to comply with the minimum security requirements, assess their effectiveness in meeting the requirement, and document the results. Any of the minimum requirements that are not met will be addressed in Step 5 where the selection of additional countermeasures will be considered.

8. STEP 4. ANALYSIS OF THREATS AND LOSSES.

a. The purpose of Step 4 is to evaluate threats and losses to determine if consideration of additional security measures to reduce the losses is required. Additional threats and vulnerabilities and resultant losses that were not fully addressed by the minimum security requirements are considered during this step. Typical threats and losses for each sensitivity level are presented in Section 4 of the Appendix; additional threats and losses not listed in Section 4 but applicable to the system should also be considered.

b. The likelihood of a threat and the potential loss that could be caused by the threat are considered and estimated on a qualitative basis (very low, low, moderate, high, very high). If the threat probability is estimated as less than moderate (low, very low) and the loss is not estimated as very high, the risk is not considered significant and security measures are not considered for the threat-loss pair. If the risk is deemed significant, security measures to comply with the requirement are selected during Step 5. The applicable threats and losses, the estimate of their probability or impact, and the determination if the risk is significant are documented to complete this step.

9. STEP 5. SELECTION OF SECURITY MEASURES.

a. Security measures are selected during Step 5 based upon the results of tasks previously completed in Steps 3 and 4. The selection includes security measures to comply with the minimum security requirements that are not met (Step 3) and to reduce the threats/losses where the risk is significant (Step 4).

b. Suggested security measures are listed in the Appendix but SRAG users may consider other security measures applicable to their operational environment. The security measures selected and the relevant requirements of Steps 3 and 4 should be documented. The security measures selected to comply with the minimum security requirements of Step 3 are used as recommendations in Step 7; the security measures selected to reduce expected losses of significant threats/losses of Step 4 will go through the cost benefit analysis process of Step 6.

10. STEP 6. COST BENEFIT ANALYSIS.

a. A cost benefit analysis of the security measures selected to respond to the threat/loss analysis of Step 4 is conducted during this step to consider their cost effectiveness and to provide the rationale and justification for recommending security measures to management for action. The security measures that are not considered cost effective based on the cost benefit analysis are dropped from further consideration. A cost benefit analysis is not conducted for security measures selected to meet minimum security requirements but cost information on these measures should be provided for the management decision process of Step 7. Work Form 9 can be used to provide security measure cost information or information on benefits of the required security measure.

b. The costs can be expressed in terms of dollars based on the cost of security hardware or software, personnel resources, or impact on the AIS operation. The expression of costs and benefits in annualized dollar terms where practical is recommended to provide management with a sound basis for a decision on implementation of security safeguards. Alternatively, the costs can be expressed in qualitative terms.

c. The benefits consist of reduction in the threat occurrence and/or loss impact and include any beneficial impact on mission operations due to increased protection of DOJ information against unauthorized disclosure, modification, and destruction, or disruption of information processing. The benefits should be identified and estimated in quantitative or qualitative terms. Similar to the cost estimates, expression of the benefits in quantitative terms of reduced annualized losses is recommended where practical. The alternative is to estimate the benefits in qualitative terms.

d. The person conducting the risk analysis must decide which of the security measures are justified based on the cost benefit analysis and forward these as recommendations for management consideration in Step 7. The results of the cost benefit analysis including the identification and estimate of costs and benefits for each security measure and the evaluation of its cost effectiveness should be documented using Work Form 9 of the Appendix.

11. STEP 7. RECOMMENDATIONS FOR MANAGEMENT DECISION.

a. The final step is to present the cost effective security recommendations to higher level management for a decision on whether to implement individual recommendations. A proposed schedule for implementing security measures should be provided where appropriate. Management must decide whether to provide the funding or personnel resources, or accept the operational impact that may be required for some security recommendations.

b. The alternative is for management to accept the risk to the security of DOJ information. For recommendations with significant budgetary impact, the management official may decide to delay implementing the recommendation until funding is available and should note this in the comments section of Work Form 10. The recommendations and supporting cost/benefit information should be clearly presented to the responsible management official and the decision documented using Work Form 10.

12. INSTRUCTIONS FOR CONDUCTING A RISK ANALYSIS USING THE SRAG.

a. The previous sections have provided a general description of the SRAG approach and the steps involved in conducting a risk analysis. This section provides instructions on how to use the detailed information in the tables, work forms, and sections of the Appendix. This portion of the SRAG also contains a flow chart of the SRAG process and includes charts showing the applicable tables, work forms, and sections depending on the sensitivity of the data processed and the type of system undergoing the risk analysis.

b. The SRAG includes sections that apply specifically to three categories of systems:

(1) PCs, except as noted below in (2).

(2) Mainframes, minicomputers, and other remotely accessed AISs, such as PCs used as file servers in a network configuration.

(3) Application systems.

c. Within the first two categories, there are sections that are applicable only if nonsensitive, sensitive, or classified data are processed. For application systems, some sections are applicable either to nonsensitive or sensitive applications.

d. In conducting a risk analysis of a system, the person conducting the risk analysis must initially determine which category and sensitivity level is applicable. Classified information includes all National Security Information (Top Secret, Secret, or Confidential) classified under Executive Order No. 12356. Sensitive (Limited Official Use) information is defined in Order DOJ 2620.7, "Control and Protection of Limited Official Use Information," as unclassified information that must be protected against release to unauthorized individuals. The term "sensitive application systems" is defined in the Definitions section of the SRAG.

e. A separate risk analysis does not have to be conducted for each individual PC. A single risk analysis can be conducted for PCs with a similar configuration and sensitivity level and located in a common physical and security environment. Also, any minor differences in individual PCs included in the risk analysis can be noted in the applicable sections and/or recommendations.

f. A flow chart of the SRAG process is contained in Figure 1 (Page 12). The risk analysis proceeds through consecutive steps from Step 1 through Step 7. The first two steps involve gathering information on the system including relevant security information. The third step consists of determining if the security measures in place effectively meet the applicable minimum security requirements. If a minimum security requirement is not met, security measures to meet the requirement are selected in Step 5 and are included in the recommendations provided to management in Step 7 for approval or disapproval.

g. Step 4 is used to consider additional threats and losses not covered by the minimum requirements and to determine if they present a significant risk. Security measures are considered in Step 5 for any threats/losses that are estimated to be a significant risk. A cost benefit analysis is performed in Step 6 to determine if the security measures are cost effective. All security measures that are justified based on the cost benefit analysis are presented as recommendations in Step 7. In Steps 4 and 5, the person conducting the risk analysis may consider other threats, losses, and security measures not listed in the SRAG.

h. The last step is used to submit all documented results of the risk analysis including the recommendations for consideration by a management official. Management either approves implementation of the recommendation or decides to accept the risk. The signatures of the person conducting the risk analysis and the management official approving/disapproving the recommendations are required to complete the risk analysis.

i. The portions of the SRAG applicable to each category and sensitivity level are shown in Figures 2, 3, and 4. These figures indicate which SRAG sections, tables, or work forms are applicable in each of the eight subcategories. In Sections 3.1, 3.2, 3.3, 5.1. 5.2, and 5.3, the nonsensitive and sensitive sections are also applicable to sensitive and/or classified processing. The person conducting the risk analysis should ensure that all work forms are appropriately completed to document the risk analysis results. It is especially important to provide the recommendations to higher level management in a form that is readily understood and lends itself to informed decision making. Additional information, such as a schedule for implementing the recommendations, should be considered where applicable.

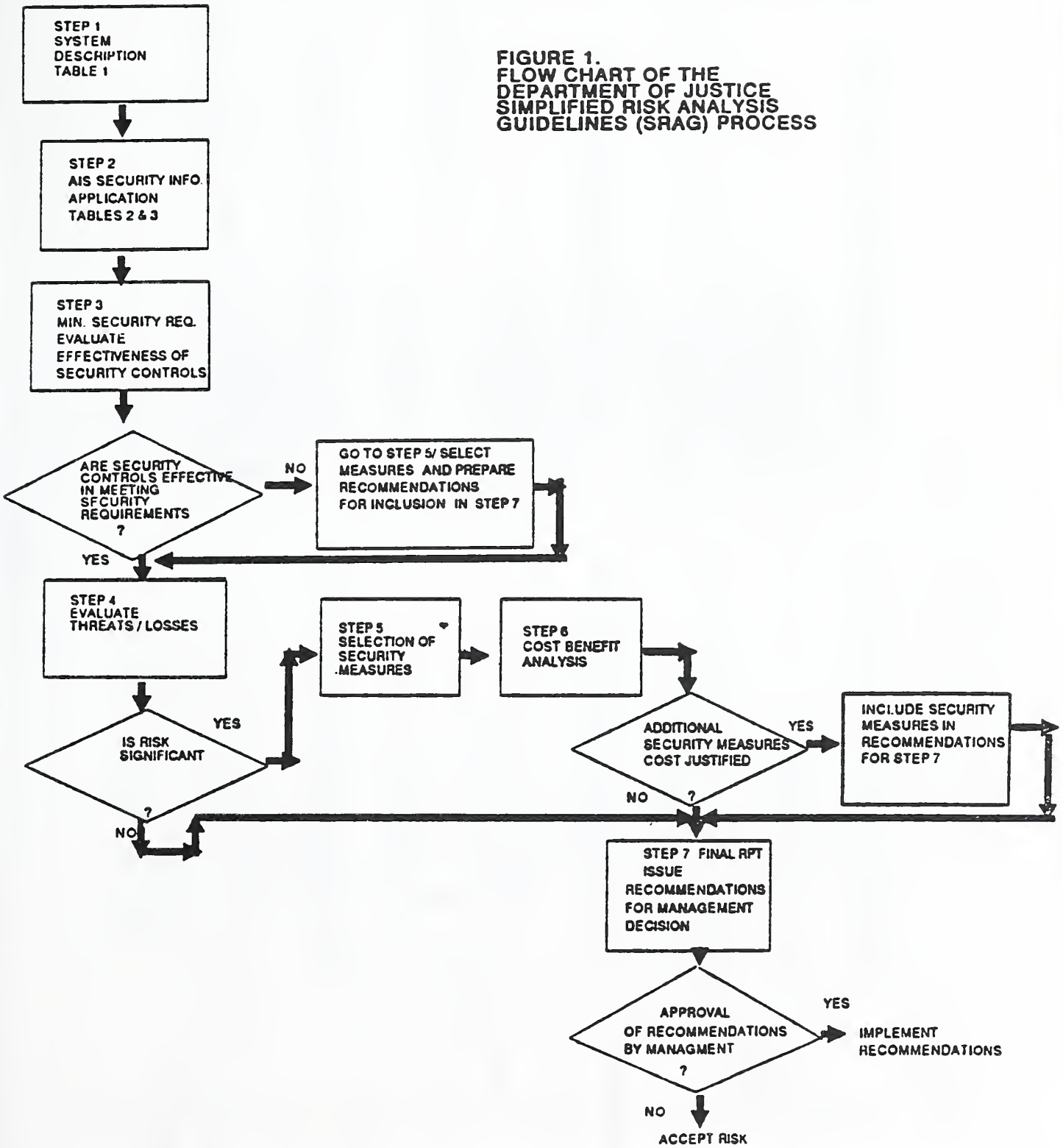


FIGURE 1.
FLOW CHART OF THE DEPARTMENT OF JUSTICE SIMPLIFIED RISK ANALYSIS GUIDELINES (SRAG) PROCESS

DEPARTMENT OF JUSTICE
SIMPLIFIED RISK ANALYSIS GUIDANCE
PERSONAL COMPUTER

TYPE OF INFORMATION	STEPS	APPLICABLE SECTIONS/TABLES	DOCUMENTED OUTPUT WORKFORM
NON-SENSITIVE	1 2 3	TABLE 1 TABLE 2 SECTION 3.1.a	WORKFORM 1 WORKFORM 2 WORKFORM 6
	4 5	SECTION 4.1.a SECTION 5.1.a, 5.4 a	WORKFORM 7 WORKFORM 8
	6 7	SECTION 6.1, TO 6.8 SECTION 7	WORKFORM 9 WORKFORM 10
SENSITIVE	STEPS	APPLICABLE SECTION/TABLES	DOCUMENTED OUTPUT/ WORKFORM
	1 2 3	TABLE 1 TABLE 2 SECTION 3.1.a, 3.1.b	WORKFORM 1 WORKFORM 2 WORKFORM 6
	4 5	SECTION 4.1.b SECTION 5.1.a, 5.1b 5.4 b	WORKFORM 7 WORKFORM 8
	6 7	SECTION 6.1, TO 6.8 SECTION 7	WORKFORM 9 WORKFORM 10
CLASSIFIED	STEPS	APPLICABLE SECTION/TABLES	DOCUMENTED OUTPUT WORKFORM
	1 2 3	TABLE 1 TABLE 2 SECTION 3.1.a, 3.1.b, 3.1.c	WORKFORM 1 WORKFORM 2 WORKFORM 6
	4 5	SECTION 4.1.c SECTION 5.1.a, 5.1b, 5.1c, 5.4 c	WORKFORM 7 WORKFORM 8
	6 7	SECTION 6.1, TO 6.8 SECTION 7	WORKFORM 9 WORKFORM 10

FIGURE 2

DEPARTMENT OF JUSTICE
SIMPLIFIED RISK ANALYSIS GUIDANCE
mainframe/mini/computer

TYPE OF INFORMATION	STEPS:	APPLICABLE SECTIONS/TABLES	DOCUMENTED OUTPUT/ WORKFORM
NON-SENSITIVE	1 2 3	TABLE 1 TABLE 2 SECTION 3.2.a	WORKFORM 1 WORKFORM 2& 4 WORKFORM 6
	4 5	SECTION 4.2.a SECTION 5.2a, 5.5.a	WORKFORM 7 WORKFORM 8
	6 7	SECTION 6.1, TO 6.8 SECTION 7	WORKFORM 9 WORKFORM 10
	STEPS:	APPLICABLE SECTION/TABLES	DOCUMENTED OUTPUT/ WORKFORM
SENSITIVE CLASSIFIED	1 2 3	TABLE 1 TABLE 2 SECTION 3.2.a, 3.2.b	WORKFORM 1 WORKFORM 2 & 4 WORKFORM 6
	4 5	SECTION 4.2.b SECTION 5.2.a, 5.2b 5.5.b	WORKFORM 7 WORKFORM 8
	6 7	SECTION 6.1, TO 6.8 SECTION 7	WORKFORM 9 WORKFORM 10
	STEPS:	APPLICABLE SECTION/TABLES	DOCUMENTED OUTPUT/ WORKFORM
CLASSIFIED	1 2 3	TABLE 1 TABLE 2 SECTION 3.2.a, 3.2.b, 3.2.c	WORKFORM 1 WORKFORM 3 & 5 WORKFORM 6
	4 5	SECTION 4.3.b SECTION 5.2.a, 5.2.b, 5.2.c, 5.5.c	WORKFORM 7 WORKFORM 8
	6 7	SECTION 6.1, TO 6.8 SECTION 7	WORKFORM 9 WORKFORM 10

FIGURE 3

DEPARTMENT OF JUSTICE
SIMPLIFIED RISK ANALYSIS GUIDANCE
APPLICATION SYSTEM

TYPE OF INFORMATION	STEPS	APPLICABLE SECTIONS/TABLES	DOCUMENTED OUTPUT/ WORKFORM
NON-SENSITIVE	1 2 3	TABLE 1 TABLE 3 SECTION 3.3.a	WORKFORM 1 WORKFORM 3 & 5 WORKFORM 6
	4 5	SECTION 4.3.a SECTION 5.3.a 5.6.a	WORKFORM 7 WORKFORM 8
	6 7	SECTION 6.1, TO 6.8 SECTION 7	WORKFORM 9 WORKFORM 10
	STEPS	APPLICABLE SECTION	DOCUMENTED OUTPUT/ WORKFORM
SENSITIVE	1 2 3	TABLE 1 TABLE 3 SECTION 3.3.a, 3.3.b	WORKFORM 1 WORKFORM 3 & 5 WORKFORM 6
	4 5	SECTION 4.3.b SECTION 5.3.a, 5.3b , 5.6.b	WORKFORM 7 WORKFORM 8
	6 7	SECTION 6.1, TO 6.8 SECTION 7	WORKFORM 9 WORKFORM 10

FIGURE 4

APPENDIX

TABLE 1

SYSTEM DESCRIPTION

1. System Name/Identification.

2. Component/User.

3. Names and phone numbers of the system manager and system security personnel.

4. Component activities or mission supported by the system.
   -Purpose of the system.

5. Type of System - Mainframe, minicomputer, wide area network, local area network, application system, personal computer.

6. System Costs.
   -Estimated cost of replacing system hardware and software.

7. Total System Configuration (Narrative and Diagram).
   -Physical location of system.
   -Connections.
   -System and application software.
   -System components, peripherals, and communications.
   -Number of users.
   -Number of application systems.
   -Description of application system(s) or major applications.
   -Methods of system access.
   -Nature of data input(s) and output(s).
   -System and application system personnel.
   -Maintenance personnel.

   Application System.
   -Purpose.
   -Description.
   -Type of data processed.
   -Where and how used.

   Personal Computers.
   -Physical location.
   -Users (single, group).
   -Connection (stand-alone, AIS, network).
   -Vendor - model, serial number.
   -Storage media (fixed, removable).
   -Application (word processing, spreadsheet).

STEP 1 SYSTEM DESCRIPTION	
1. SYSTEM NAME	2. COMPONENT/USER
3. SYSTEM MANAGER/PHONE	4. PURPOSE
5. SYSTEM TYPE	6. SYSTEM REPLACEMENT COST $
7. SYSTEM CONFIGURATION (NARRATIVE)	

WORKFORM 1
SYSTEM DESCRIPTION

TABLE 2
AIS SECURITY INFORMATION

Prepare a narrative considering the following items:

1. Description of Sensitivity and Criticality of Data Processed.
   -Based on Tables 2 & 3.
   -Threats to data.

2. Risk Analysis (RA).
   -Date of last RA.
   -Person or contractor conducting RA.
   -Methodology used.
   -Action taken on recommendations.
   -RA documentation.

3. Contingency Plans (CPs).
   -Emergency response, back-up, and recovery for large systems.
   -Status of plans.
   -Documentation of CP.
   -Used or tested (date).

4. Description of Security Measures.

   a. Physical Security.
      -Locks, guards, detection systems.
      -Fire and environmental hazards.

   b. Personnel Security.
      -Background investigations.
      -Security clearances.

   c. Administrative Procedures.
      -Issuance of implementing security directives.
      -Documented security plan.
      -Restrictions on activities of users, programmers, etc.
      -Separation of duties for critical functions.
      -Security awareness program.

   d. Software Security Controls.
      -User identification and authentication.
      -Audit trails.
      -File access authorization.
      -Dial back.
      -Restriction on unsuccessful access attempts.
      -File encryption.

   e. Technical Security.
      -Encryption of communications.
      -Tempest products.

STEP 2

AIS SECURITY INFORMATION

DESCRIPTION OF SENSITIVITY	DESCRIPTION OF CRITICALITY

STATUS OF RISK ANALYSIS

STATUS OF CONTINGENCY PLANS (NARRATIVE)

DESCRIPTION OF SECURITY MEASURES IN PLACE

WORKFORM 2
AIS SECURITY INFORMATION

TABLE 3
DATA SENSITIVITY

Prepare an inventory of all application systems addressing the following items for each application:

1./2. Name/Owner of Application.

3. Component(s) Supported - Number of Users, Data Quantity.

4. Purpose of Application System.

5. How is the Application Accessed, Updated?

6. Determine Data Sensitivity Level (National Security Information, Limited Official Use, Nonsensitive).

   a. National Security Information (Confidential, Secret, Top Secret).

   b. Limited Official Use Information: (Sensitive)
      - Informant and witness information.
      - Grand Jury information subject to Federal Rules of Criminal Procedure, Rule 6(e), "Grand Jury Secrecy of Proceedings and Disclosure."
      - Investigative material.
      - Law enforcement information.
      - Tax information subject to 26 U.S.C Section 6103, "Publicity of Returns and Disclosure of Information as to Persons Filing Income Tax Returns."
      - Information that could be sold for profit.
      - Personal information subject to The Privacy Act of 1974.
      - Information that discloses security vulnerabilities.
      - Information that could result in physical risk to individuals.
      - Company proprietary information.
      - Deliberative information relating to internal DOJ or Executive Branch policy and decision making.

7. Description of threats to the disclosure, modification, destruction, and availability of system data.

8. Description of losses if data is disclosed, modified, or destroyed in an unauthorized manner, or if processing of application is interrupted.

9. Prioritized application systems by sensitivity and criticality for large AISs to the extent practical.

STEP 2

DATA SENSITIVITY

1. NAME OF APPLICATION

2. CUSTODIAN OF APPLICATION

3a. COMPONENT(S)

3b. ESTIMATED NUMBER OF USERS

3c. DATA QUANTITY

4. PURPOSE OF APPLICATION

5. DESCRIBE METHODS OF ACCESSING APPLICATION

6. DATA CLASSIFICATION

☐ NATIONAL SECURITY INFORMATION

☐ LIMITED OFFICIAL USE (LOU) INFORMATION DESCRIBE TYPE

7. DESCRIBE THREATS TO DISCLOSURE, MODIFICATION, AND DESTRUCTION OF DATA

8. DESCRIBE CONSEQUENCE OF LOSS, MODIFICATION, OR DESTRUCTION OF DATA

9a. STATE SENSITIVITY LEVEL OF APPLICATION

9b. STATE CRITICALITY OF APPLICATION

WORKFORM 3

APPLICATION SYSTEM DATA SENSITIVITY

STEP 2

AUTOMATED INFORMATION SYSTEM FACILITY (AIS)

PRIORITIZATION OF APPLICATION SYSTEMS

9A. APPROXIMATE RANKING OF SENSITIVITY OF APPLICATION SYSTEMS PROCESSED AT THE AIS FACILITY.

9B. RANK CRITICALITY LEVEL OF EACH APPLICATION WITH RESPECT TO THE FUNCTIONS EACH AIS APPLICATION SUPPORTS.

WORKFORM 4

PRIORITIZATION OF SENSITIVITY AND CRITICALITY OF APPLICATIONS

STEP 2
CRITICALITY OF APPLICATION SYSTEM

Component _____

Application Name _____

System Owner _____

Criticality of Application (please check one)

Vital	_____	The organization could not accomplish its mission without the application.
Important	_____	The application is necessary for the organization to perform its mission in a cost-effective and timely manner.
Useful	_____	The application improves productivity or saves costs but is not essential to operations.

Estimate of impact on organization if processing of application is interrupted for various periods of time. Application system owners are requested to estimate the loss if the application cannot be processed for the periods of time listed. The loss estimate should consider the impact on mission operations, the cost of using a manual back-up system, any idle manpower or equipment, and losses in the effectiveness and efficiency of the DOJ project. Please estimate the losses for each delay listed (hour to one month) as I, L, M, H, or C considering the following:

I - Insignificant (less than $1,000).
L - Low ($1,000 to $10,000).
M - Moderate ($10,000 to $100,000).
H - High ($100,000 to $1,000,000).
C - Catastrophic (over $1,000,000).

1 Hour	_____	1 Day	_____	2 Weeks	_____
2 Hours	_____	2 Days	_____	1 Month	_____
4 Hours	_____	1 Week	_____		

Have plans been developed to process the application system elsewhere if processing is interrupted? Yes ____ No ____
If yes, describe the plans.

_____

_____

STEP 3
MINIMUM REQUIREMENTS

3.1. Microcomputers/Personal Computers (PCs). This section is applicable to all PCs except PCs used as file servers or as part of a "network" where its data can be accessed from remote locations. Those PCs are subject to the minimum security requirements of Section 3.2 of the Appendix.

a. Nonsensitive Processing.

(1) Physical security controls to protect the PC from theft or tampering are required.

(2) Files critical to the PC owner must be backed up and stored apart from the immediate work area.

(3) Activities such as eating, drinking, or smoking are not permitted while using the PC.

b. Sensitive Processing. In addition to the security requirements listed for nonsensitive processing on PCs, the minimum security requirements listed below are required for sensitive processing.

(1) Physical access to the PC location will be controlled and limited to authorized users. Physical security measures such as dead bolt locks for PC area doors are recommended.

(2) If highly sensitive data are processed, the use of removable storage media for storing the data is required. The removable media must be stored in a security container or locked file cabinet after normal working hours.

(3) PCs used as remote work stations must be turned off, disabled, or disconnected from the system after normal working hours.

(4) If a PC is connected to an AIS or network, the AIS/network must provide for the unique identification and authentication of system users and an audit trail that enables the reconstruction, review, and examination of a sequence of security related events.

(5) Contingency plans are required to provide for the continuity of data processing in the event that the PC cannot be used for processing.

(6) Training in computer security awareness and computer security measures/procedures is required for all PC users.

(7) Each system user shall be informed of the responsibility to report any security related events to the component's Security Programs Manager (SPM) or the AIS security officer.

(8) If classified data are inadvertently written on fixed storage media, the media must be sanitized by writing any pattern of binary ones and zeros into the memory locations containing the classified data.

c. Classified Processing. In addition to the security requirements listed for nonsensitive and sensitive processing on PCs, the minimum security requirements listed below are required for classified processing.

(1) A system security plan for the AIS must be developed to include a system description, access controls, software security controls, security measures and responsibilities, and other security related information. The plan will include procedures in effect such as a prohibition of the system for nonwork related activities and a prohibition of the use of nonapproved software and privately owned equipment for classified processing. A master AIS security plan may be developed for a number of PCs used in a similar environment to process classified information.

(2) The system must be accredited by the Department Security Officer (DSO), the component's SPM, or their designees to process classified information. If foreign intelligence is involved, a National Foreign Intelligence Board (NFIB) member, or person delegated by the member will accredit the system. A single accreditation action may be used to accredit a large number of PCs operating under a master AIS security plan.

(3) Personnel authorized to use the PC must be cleared to the highest level and most restrictive category of classified material contained in the system.

(4) The implementation of extensive security procedures is required if a PC processing classified information is also used as part of an unclassified AIS or network. The procedures that must be implemented include the use of a physical switch to remove the computer from the network during classified processing and the sanitization or removal of all storage media prior to the beginning, and at the end, of classified processing. The detailed procedures are required to be included in the AIS security plan.

(5) Physical protection for a PC, which uses fixed nonvolatile storage media for storage of classified information, must be commensurate with the highest level of classification and most restrictive category of classified material contained in the system. Classified information cannot be stored on fixed media unless the area is approved for open shelf storage of classified information.

(6) Maintenance personnel requiring access to portions of the system that affect security, or who will have access to classified information, shall be cleared to the highest level and most restrictive category of classified material contained in the system. Uncleared maintenance personnel requiring access to the system must be escorted by appropriately cleared DOJ personnel and the access must be preceded by removal of all classified information from the system and the work place.

(7) Classified output must be appropriately marked and handled only by authorized individuals.

(8) Media used for processing classified information must display an external label indicating the highest level of classification assigned the data currently or previously stored on the media.

(9) When the PC area is unattended, media containing classified data must be stored in an approved security container.

(10) Contingency plans must ensure that copies of files, documentation, and other materials essential to recovery and continued processing are stored apart from the PC work area and that the back-up PC is approved for the same or a higher level of classified processing.

(11) The copying or use of utility or other programs from bulletin boards or other nonvendor sources is prohibited.

(12) Nonvolatile storage media containing classified information cannot be removed from the area by PC maintenance personnel unless the media has been properly sanitized.

(13) Communication circuits interconnecting PCs that process or store classified information must be secured by the use of cryptographic devices approved by the National Security Agency (NSA) for protecting classified information. Modems used with PCs should be turned off except when needed to transfer data.

(14) When no longer useful, storage media containing classified data must be sanitized and/or destroyed in accordance with applicable national policy directives.

3.2. Mainframes, Minicomputers, and Other Remotely Accessed AISs.

a. Nonsensitive Processing.

(1) The responsibility for security of the AIS shall be assigned to an individual designated as the Automated Information System Security Officer (AISSO). The AISSO is responsible for establishing, directing, and maintaining an AIS security program.

(2) An AIS security plan must be developed and maintained to identify the security features of the AIS and all applicable directives, laws, and circulars. The plan will also describe the degree of compliance with applicable AIS security requirements and provide for its revision whenever significant system changes are made that have an impact on security. The plans should be more extensive if sensitive and/or classified information is processed by the system.

(3) Access to the AIS facility shall be controlled by physical security measures and/or administrative procedures.

(4) The AIS shall provide the capability to uniquely identify each individual system user, associate this identity with all auditable actions taken by that individual, and provide a mechanism to authenticate the user's identity. The user identification and authentication process must comply with the DOJ order, Unique Identification and Authentication of Users of Automated Information Systems. Passwords used for authentication must comply with the requirements of FIPS 112, Standard for Password Usage.

(5) Fire and water protection measures shall be implemented to protect personnel and system resources.

(6) Contingency plans, which provide reasonable continuity of data processing support when normal operations are disrupted, are required and should include plans for emergency response, back-up operations, and recovery. The portions of the contingency plans affecting applications systems processed at the AIS installation should be provided to application system managers.

(7) A risk analysis of the AIS shall be conducted at least once every five years and documented. A risk analysis is required prior to the approval of design specifications for new AIS installations and whenever significant changes occur to the installation.

(8) Implementation of security measures to achieve system integrity is required.

b. Sensitive Processing. In addition to the requirements for nonsensitive processing, the following additional requirements must be met if sensitive data are processed by the AIS:

(1) DOJ employees requiring unescorted access to the AIS facility and users handling sensitive data shall have clearances issued under Executive Order 10450, "Security Requirements for Government Employment," based on a full-field background investigation.

(2) Physical security measures such as locks, alarms, and/or guards shall be implemented for the AIS facility.

(3) The AIS shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the system files, programs, and data. (This requirement and the requirements listed in succeeding paragraphs 4 and 5 can be met by implementing a software security system that meets the C2 requirements of the Department of Defense Trusted Computer System Evaluation Criteria or "Orange Book.")

(4) The AIS shall assure that storage space, allocated to a system user, does not contain any data for which the user is not authorized.

(5) Security measures, such as administrative procedures and/or hardware and software controls, shall be implemented to control access to sensitive data.

c. Classified Processing. In addition to meeting the minimum security requirements for nonsensitive and sensitive processing for mainframes, minicomputers, and other remotely accessed AISs listed above, the minimum security requirements listed below must be met if the AIS processes classified information.

(1) A system security plan, which will identify all actions to be taken to implement or modify the security features of the system and all applicable regulations, must be developed and maintained. The plan will describe the required degree of compliance to the security requirements and provide for review and revision as appropriate whenever system changes are made that have an impact on security.

(2) The DSO or the component's SPM shall accredit the AIS to process classified information in a specified mode of operation. Approval of the DSO is required to process in the compartmented or multilevel mode. The system accreditation document will identify the authorized mode of operation, the types of information processed by the system, the system's approved direct and indirect users, and the security safeguards in effect. The accreditation will be based on an evaluation of the AIS security measures and a certification by the AIS security officer that the system meets the security requirements for processing classified information. An AIS processing foreign

intelligence information must be accredited by an NFIB member or an individual designated by the member.

(3) Storage media will be physically controlled and safeguarded in a manner commensurate with the highest classification of data ever recorded thereon until approved destruction of the media or execution of approved sanitized procedures.

(4) Removable information storage media will bear external labels indicating the security classification of the information and applicable handling caveats and dissemination control labels.

(5) The system must mark each page of all human-readable hard copy output with the classification and the dissemination and handling caveats of the information processed.

(6) The communications links connecting the components of the AIS must be encrypted using encryption devices approved for the classification level of the system data.

(7) The AIS must be in compliance with the appropriate national policy on compromising emanations.

(8) The AIS and all central and remote facilities housing equipment attached thereto will comply with the applicable standards for physical protection of the data processed therein.

(9) Personnel operating AIS equipment at the central site and all users at remote locations must be cleared, approved for access, and have appropriate need-to-know approvals for the data processed by the AIS.

(10) All routine on-site maintenance functions performed by hardware and systems software specialists must be performed by personnel who have been cleared and approved for access at the highest level of information that the system has been accredited to process.

3.3. Application Systems.

a. Nonsensitive.

(1) A management control process shall be established to assure that appropriate administrative, physical, and technical safeguards are incorporated into all new applications, and into significant modifications to existing applications.

(2) The AIS shall control the capability to input, update, or change system data and restrict this capability to specified authorized individuals or groups.

(3) Security measures to validate data must be implemented.

(4) All system users shall be uniquely identified and authenticated.

b. Sensitive. In addition to the requirements for nonsensitive application systems listed above, the minimum security requirements listed below for sensitive application systems must be met.

(1) Security requirements and specifications must be defined and approved by the application system manager prior to acquiring or starting formal development of the application. Prior to placing the application in operation, design reviews and system tests shall be conducted to assure that the proposed design meets the security specifications.

(2) Upon completion of the system tests, the application system manager must certify that the system meets all applicable Federal policies, regulations, and standards, and that the results of the tests demonstrate that the installed security safeguards are adequate for the application.

(3) Contingency plans must be developed to assure that users can continue to perform essential functions in the event their data processing support is interrupted. The plans should be consistent with the contingency plans of the AIS installation that is processing the application.

(4) The AIS shall control access to system data using access control lists of individuals or groups authorized to access system files, programs, or data.

(5) An audit trail is required to maintain a record of accesses and attempted accesses to system data.

(6) If an application is used to process classified data, the AIS must comply with all applicable policy directives.

STEP 3 MINIMUM SECURITY REQUIREMENTS		
REQUIREMENT	MEASURE IN PLACE	SECURITY MEASURE COMPLIANCE

WORKFORM 6
MINIMUM SECURITY REQUIREMENTS

STEP 4
ANALYSIS OF THREATS AND LOSSES

4.0. Introduction.

a. The security objectives that should be considered are listed below along with the threats and losses that must be evaluated to determine if the risk is significant. If the risk is deemed significant, security measures to achieve the security objective should be considered to reduce the threat or to reduce the impact of the loss. If the risk is not significant, the threats/losses are not considered further. The suggested security measures to achieve each of the security objectives are listed in Step 5.

b. The likelihood of the threat occurring should be evaluated and estimated on a qualitative basis as very low, low, moderate, high, or very high. Similarly, the impact of the loss should be evaluated on the same qualitative basis. The threat and loss estimates should be documented in Work Form 7. The risk will be considered as significant if either of the following conditions exist:

(1) The threat probability is rated as moderate or higher.

(2) The loss is estimated as very high.

c. As stated previously, the security objectives that have significant risks associated with them and require consideration of security measures should be noted and addressed during Step 5 of the SRAG process. The security objectives and the threats and losses that require evaluation are listed below in Sections 4.1, 4.2, and 4.3. The person conducting the risk analysis should also consider other threats/losses that impact on their system but are not listed.

4.1. PCs.

a. Nonsensitive Processing.

(1) Physical Control of Access to PC.
Threat - Access to PC by unauthorized users.
Loss - Data disclosure, modification, or destruction, or equipment loss.

(2) Procedures to Remove PC From Network/System. (applicable if PC is connected to a network or system).
Threat - Access from remote site during nonduty hours.
Loss - Data disclosure, modification, or destruction.

(3) Software Security for PCs in a Network/System (applicable if PC is connected to a network or system).
Threat - Unauthorized access to system/network data.
Loss - Disclosure, modification, or destruction of system/network data.

(4) Contingency Plans to Identify a Back-Up PC.
Threat - Termination of processing if PC fails.
Loss - Processing capability for critical applications.

(5) Surge Suppressors to Reduce Power Fluctuations.
Threat - Power "spikes" to destroy data or equipment.
Loss - Data loss or equipment failure.

b. Sensitive Processing.

(1) Background Checks of Maintenance Personnel.
Threat - Access to data or insertion of viruses.
Loss - Data disclosure, modification, or disclosure.

(2) Identifying Media Containing Highly Sensitive Data.
Threat - Inadequate protection of storage media.
Loss - Data on storage media.

(3) Storage of Media Containing Highly Sensitive Data.
Threat - Theft or loss of storage media.
Loss - Data on storage media.

(4) Back-Up of Files and Documentation Outside PC Area.
Threat - Disaster destroying PC and storage media.
Loss - Loss of data if disaster occurs.

(5) Security Procedures Restricting Copying of Programs. From Unauthorized Sources.
Threat - Introduction of a virus.
Loss - Data destruction or loss of PC use.

(6) Sanitization of Storage Media Prior to Their Removal.
Threat - Access to data during maintenance of media.
Loss - Disclosure of sensitive data.

(7) Encryption of PC Communications.
Threat - Interception of data communications.
Loss - Disclosure of sensitive data.

(8) Encryption of Data to Hard Disk.
Threat - Access to data on hard disk.
Loss - Disclosure of sensitive data.

(9) User Identification and Authentication.
Threat - Use of PC by unauthorized personnel.
Loss - Data disclosure, modification, destruction.

(10) Audit Trail of PC Use.
Threat - Unauthorized PC use.
Loss - Failure to detect unauthorized PC use.

(11) Surge Suppressors to Reduce Power Fluctuations.
Threat - Power "spikes" to destroy data or equipment.
Loss - Data loss or equipment failure.

c. Classified Processing.

(1) Tempest Threat.
Threat - Obtaining information through emanations.
Loss - Disclosure of classified data.

(2) Encryption of Data to Hard Disk
Threat - Access to data on hard disk.
Loss - Loss of classified data if hard disk used.

(3) User Identification and Authentication.
Threat - Use of PC by unauthorized personnel.
Loss - Modification or destruction of operating system and/or proprietary software. Loss of data.

(4) Audit Trail of PC Use.
Threat - Unauthorized PC use.
Loss - Failure to detect unquthorized PC use.

(5) Surge Suppressors to Reduce Power Fluctuations.
Threat - Power "spikes" to destroy data or equipment.
Loss - Data loss or equipment failure.

4.2. Mainframes, Minicomputers, and Other Remotely Accessed AISs.

a. Nonsensitive Processing.

1. Physical Security Protection for AIS Facility.
Threat - Unauthorized physical access to facility.
Loss - Theft or destruction of equipment, data.

2. Record of System Accesses.
Threat - Inability to track access to system resources.
Loss - Deterrent impact on unauthorized accesses.

b. Sensitive Processing.

(1) Documentation of Security Features.
Threat - Failure to implement/use security measures.
Loss - System resources.

(2) Communication Lines.
Threat - Interception of data communications.
Loss - Data disclosure.

(3) Background Investigation for On-Site Hardware/Software.
Maintenance Personnel.
Threat - Access to data during routine maintenance.
Loss - Disclosure of data.

4.3. Application Systems.

a. Nonsensitive.

(1) Contingency Plans.
Threat - Hardware failure, loss of utilities.
Loss - Inability to process application.

(2) Access Control.
Threat - Unauthorized access to data.
Loss - Data modification or destruction.

(3) Audit Trail.
Threat - Unauthorized use of system resources.
Loss - Deterrent factor and ability to trace usage.

b. Sensitive.

(1) Separation of Duties.
Threat - Fraud of applications controlling assets.
Loss - Money, supplies, equipment, or other assets.

STEP 4

ANALYSIS OF THREATS AND LOSSES

THREAT	PROBABILITY OF OCCURRENCE	LOSS	ESTIMATE OF IMPACT OF LOSS	IS RISK SIGNIFICANT

WORKFORM 7
ANALYSIS OF THREATS AND LOSSES

STEP 5
SELECTION OF SECURITY MEASURES

The following security measures listed in Sections 5.1, 5.2, and 5.3 are examples of measures that should be considered to comply with the minimum security requirements of Sections 3.1, 3.2, and 3.3. The security measures should be documented on Work Form 8.

5.1. PCs.

a. Nonsensitive Processing.

(1) Physical devices to lock PCs to desks, tables, etc. to prevent PC from being easily removed from area. Locks, preferably dead bolt, on doors to PC area.

(2) Backing up critical files on media, such as floppy disks, which should preferably be stored outside the PC working area.

(3) Issuing operating procedures for PC users which include prohibiting eating, drinking, or smoking while using the PC.

b. Sensitive Processing.

(1) Dead bolt locks on PC area doors. Building controls such as 24-hour guard service or locked doors for controlling access to floors or controlled areas. Locating PCs so that personnel in area could observe unauthorized PC users.

(2) Use of removable storage media for highly sensitive data. Media should be stored in a locked file cabinet or safe at the end of the working day.

(3) At a minimum, PCs should be turned off at the end of the working day. Preferably, the AIS should disable or disconnect the PC unless notified by an authorized user that continued use of the AIS is required.

(4) The AIS must provide for the unique identification and authentication of PC users and an audit trail.

(5) Alternate compatible PCs with similar features and security controls, which are available for use, should be identified. Files and essential programs should be backed up.

(6) Security awareness training, such as formal training courses, security pamphlets, brochures, and video cassettes, and issuance of security policy, procedures, and awareness memoranda, should be available to all PC users.

(7) & (8) Issuance of security procedures to all PC users informing them of the need to contact security personnel to report security related incidents and to sanitize any fixed storage media that inadvertently contains classified information.

c. Classified Processing.

(1) Document system security plan for the AIS.

(2) Documentation of accreditation action by the responsible management official based on the AIS security plan.

(3) Authorized PC users must have appropriate security clearances and access approvals where required.

(4) Implementation of security procedures for switching to/from the use of the PC for classified processing.

(5) An approved secure area or the use of removable storage media or encryption of data on hard disk using approved encryption techniques.

(6) Issuance and implementation of security procedures for maintenance personnel.

(7) Access to classified output must be restricted to individuals with the appropriate security clearances. The classified output should be stamped manually with the appropriate security classification if the system does not provide automated classification markings on its output.

(8) Affix label to storage media.

(9) Implement security procedure for storing media to prevent access to classified data on the media.

(10) Include procedures for storage of critical files and the selection of alternate back-up PCs in the PC contingency plans and implement procedures.

(11) Issue security procedures to reduce virus threat.

(12) Implement security procedures to sanitize storage media by overwriting or degaussing prior to release of media for maintenance.

(13) Use crypto equipment approved for classified information when using communication circuits.

(14) Implement security procedures to sanitize, degauss, and/or destroy storage media prior to its release. Security Programs Managers or the SEPS should be contacted for assistance in complying with the minimum requirements of (12) or (14).

5.2. Mainframes, Minicomputers, and Other Remotely Accessed AISs.

a. Nonsensitive Processing.

(1) Assign responsibility for the AISSO function.

(2) Develop an AIS security plan which identifies security features of the AIS and plans to comply with minimum security requirements.

(3) Implement security measures such as building guards, AIS facility and area locks, badges, card readers, AIS facility authorized access list, and sign-in sheets for nonauthorized personnel.

(4) Implement a system to provide each user with a unique user identifier and authenticator (e.g., password). If passwords are used, they must comply with FIPS 112, "Password Usage".

(5) Implement smoke detection, sprinklers, portable fire extinguishers, water drains and detectors, and/or fire suppression systems.

(6) Develop contingency plans for the AIS facility using applicable DOJ and FIPS PUBs for guidance.

(7) Conduct a risk analysis at least every five years or when significant changes occur in the AIS operation using SRAG and applicable FIPS PUBs as guidance and document the results.

(8) Implement security measures such as controls on AIS hardware/software changes, testing of new and modified software, and fault detection systems.

b. Sensitive Processing.

(1) Ensure that DOJ personnel requiring unescorted access to the AIS installation have E.O. 10450 full field background investigations. Issue procedures requiring DOJ users that handle sensitive data to have similar background investigations.

(2) Provide adequate locks, cardkey system, guards, badges, and alarms to control access to the AIS facility.

(3) (4) & (5) The three requirements can be met by using a software security product that meets the C2 rating requirements of the Department of Defense Trusted Computer System Evaluation Criteria or "Orange Book." The product must be properly implemented in the AIS to comply fully with the requirements of Paragraphs 3.2.b.3, 3.2.b.4, and 3.2.b.5. Alternatively, software products can be implemented that the AISSO has determined meets the three requirements.

(6) Additional security measures such as hardware identification of PCs used to remotely access AISs and dial back modems should be considered to control access to sensitive data on the AIS.

c. Classified Processing.

(1) Develop a security plan for the AIS.

(2) Develop a system accreditation plan identifying the mode of operation, types of information processed, list of approved direct and indirect users, and the security safeguards. The AIS must be accredited by the appropriate accrediting authority prior to the AIS processing classified information.

(3) Implement procedures to provide physical security protection for storage media commensurate with the classification of the data stored on the media.

(4) Label all removable storage media with appropriate classification and access approval/handling caveats.

(5) Mark each page of classified output with appropriate markings either by automated or manual means.

(6) Provide NSA approved encryption devices to protect all communications links.

(7) Comply with the current Tempest policy by identifying the planned AIS location, the type and volume of classified information processed by the AIS, and the zone of control, and obtaining a review of the AIS installation by a certified Tempest technical authority.

(8) Provide physical protection for the AIS and remote facilities commensurate with the level of data processed.

(9) Implement procedures to ensure that AIS facility personnel and users have appropriate clearances and need-to-know for the data processed by the AIS.

(10) Implement procedures to ensure that AIS hardware and software maintenance personnel operating at the AIS site have appropriate security clearances.

5.3 Application Systems.

a. Nonsensitive.

(1) Implement a management control process for all new applications and for existing applications when significant changes occur.

(2) Provide software security or administrative controls to maintain data integrity by restricting the modification of data to authorized users.

(3) Implement administrative and software controls to validate data.

(4) Ensure that all application system users are uniquely identified and authenticated. If the responsibility is delegated by the Central Security Administrator, the Application System Manager is responsible for the control of user identifiers and passwords as specified in the applicable DOJ order.

b. Sensitive.

(1) For all new applications and significant changes to existing applications, implement process to ensure that security specifications are defined, and design reviews and system tests are conducted.

(2) For applications requiring implementation of the procedures of the preceding paragraph, provide document signed by the Application System Manager certifying that the system meets all applicable policies and that security safeguards are adequate for the application.

(3) Develop contingency plans for continuing essential functions when processing is interrupted considering factors such as using available manual systems or use of alternative AISs for processing application.

(4) Ensure that the AIS implements software security controls to restrict access of sensitive data to authorized users.

(5) Ensure that the AIS implements an audit trail to record accesses and attempted accesses to application data.

(6) If the application will process classified data, ensure that security controls to comply with the requirements of Section 3.2.c for processing classified data are implemented by the AIS.

(The following security measures listed in Sections 5.4, 5.5, and 5.6 should be considered to meet the security objectives of Sections 4.1, 4.2, and 4.3 which have been determined to have significant risk during Step 4. Other security measures may also be considered and the results documented using Work Form 8.)

5.4 PCs.

a. Nonsensitive Processing.

(1) Physical security controls for building, floor, and PC area including guards, locks on PC area doors, and control of access to PC by personnel in area.

(2) Turning off of power to PC or disconnect by AIS after normal working hours.

(3) Identification and authentication of users, access control to files, and audit trails as required by system/network.

(4) Identify a compatible PC that can be used in an emergency when the PC is unable to operate.

(5) Install surge suppressors.

b. Sensitive Processing.

(1) Require personnel background checks, such as a National Agency Check with Inquiries for maintenance personnel.

(2) Use of an external label identifying storage media as containing sensitive data.

(3) Store removable storage media in a security container or locked cabinet when PC area is unattended.

(4) Back-up critical files, documentation, and programs in a location outside the PC working area.

(5) Issuance of security procedures to restrict copying of programs from unauthorized sources.

(6) Implement security procedures to sanitize storage media whenever media is removed from the PC area and released to vendor service personnel. Contact the SEPS or the Security Programs Manger for assistance.

(7) Use encryption equipment approved for sensitive or classified processing.

(8) Install software security package to encrypt data stored on hard disk.

(9) Install software security package to identify and authenticate PC users.

(10) If PC is used by multiusers and user authentication is in effect, install an audit trail software security package.

(11) Install surge suppressors.

c. Classified Processing.

(1) Use equipment that reduces emanations to an acceptable degree and complies with Tempest requirements. Equipment on the Preferred Products List should be considered.

(2) Install software security package with NSA approved encryption to encrypt data on hard disk.

(3) Install software security package to identify and authenticate PC users.

(4) Install audit trail software only if PC users are authenticated.

(5) Install surge suppressors.

5.5 Mainframes, Minicomputers, and Other Remotely Accessed AISs.

a. Nonsensitive Processing.

(1) Provide adequate locks, cardkey system, guards, badges, and alarms to control access to the AIS facility.

(2) Install audit trail software to record use of system resources.

b. Sensitive Processing.

(1) Develop a document describing the security features of the AIS and distribute to appropriate personnel.

(2) Encrypt communications lines.

(3) Require full field background investigations for all on-site hardware and software maintenance personnel.

5.6 Application Systems.

a. Nonsensitive.

(1) Develop contingency plans considering available manual systems for application data or use of alternative AISs for processing application.

(2) Ensure that AIS processing application installs access control software to restrict changes to protect application data.

(3) Ensure that AIS maintains a system audit trail.

b. Sensitive.

(1) Implement separation of duties, where there is effective independent checking on functional activities, for the functions involved in handling the input and output of data for the application.

STEP 5 SELECTION OF SECURITY MEASURES			
SECURITY REQMT/OBJECTIVE (STEP3)	(STEP4)	SECURITY REQUIREMENT OR OBJECTIVE	RECOMMENDED SECURITY MEASURE

WORKFORM 8
SELECTION OF SECURITY MEASURES

STEP 6
COST BENEFIT ANALYSIS

6.1. A cost benefit analysis provides a cost justification for the recommendations based on the principle that the cost of the recommended security measures is less than the benefits in increased security and reduced potential losses to the system. The security measures that can be cost justified are forwarded to upper level management along with any minimum security requirements that are not effectively met to allow management to decide whether to implement the security measure or accept the risk.

6.2. The costs include the nonrecurring costs of procuring and implementing the security devices, software, etc., and the annual costs of operating and maintaining the security safeguard. Indirect costs, such as adverse impact on operational activities or additional personnel resource requirements, are frequently the only costs associated with administrative procedures and should also be considered.

6.3. The cost should be stated in annualized quantitative terms where possible, especially if dollar costs to purchase the equipment, device, or software can be identified. The life cycle costs can be annualized by adding the nonrecurring procurement and implementation costs of the security measure to the maintenance and operational costs for its expected useful life and dividing by the number of years of useful life. As an example, if a device can be purchased for $25,000, will cost $3,000 a year to maintain, and is expected to last five years, the annual cost would be ($25,000 + $15,000) $5,000 or $8,000 per year. If the cost is the additional time that personnel must apply to implement security procedures, the cost can generally be stated in quantitative terms of dollars per year.

6.4. If the cost is the impact on operations or other effects that cannot be easily quantified, it should be expressed in qualitative terms (major, moderate, minor) accompanied by a narrative description where feasible. The primary objective is to identify the costs in terms that upper level management can understand and use in deciding whether to approve the expenditure of resources.

6.5. The security measure benefits of increased security and reduced potential system losses can also include indirect benefits, such as increases in management control of system resources, compliance with national directives, security for sensitive DOJ operational activities, and executive or congressional support. The direct benefits can be expressed as the reduction in the threat probability, the increase in effectiveness of a security control, or the reduction in the impact of a loss caused by the threat.

6.6. The benefits of a security measure should be expressed in quantitative terms of reduction in annual loss expectancy if reliable estimates can be assigned to the threat/loss parameters affected by the implementation of the security measure. An estimate of the annualized loss expectancy based on the probability of a threat occurring during the year and the estimate of the loss incurred by a component due to the threat (annual loss expectancy = threat probability x loss) is required prior to quantifying the benefit of a security measure. For example:

a. If the annualized loss expectancy is $5,000 based on a threat occurring twice per year and a loss of $2,500, and

b. The threat can be reduced by 75% to 0.5 or once every two years based on implementation of a security measure.

c. The benefit is $5,000 - $1,250 or $3,750.

6.7. In many cases where quantifying the benefit is difficult, the direct and indirect benefits of a security measure can be expressed in terms of its impact on reducing expected losses or favorable impact on DOJ mission objectives while using qualitative terms to describe the impact.

6.8. The person conducting the risk analysis should evaluate the cost benefit information to determine if the security measure is cost effective and document the results on Work Form 9. Cost effective security measures should be included in the list of recommendations for consideration/action by higher level management. The cost benefit information should also be available and used as a basis for a decision by management to implement the security measure or to accept the risk. For security measures recommended to comply with minimum security requirements of Section 3, Work Form 9 may be used to provide cost and benefit information to management although the estimate of benefit and evaluation of cost effectiveness portions of Work Form 9 are not applicable and should not be completed.

STEP 6 COST BENEFIT ANALYSIS					
SECURITY MEASURE	COST DESCRIPTION	ESTIMATE OF COST*	BENEFIT DESCRIPTION	ESTIMATE OF BENEFIT*	COST EFF

* Estimate of cost and benefits may be in quantitative or qualitative terms.

WORKFORM 9
COST BENEFIT ANALYSIS

STEP 7
RECOMMENDATIONS FOR MANAGEMENT DECISION

7.1 The risk analysis should be documented by completing the work forms listed in the SRAG appendix and concluding with Work Form 10 which includes a list of security recommendations for consideration by a senior management official. Additional information on the recommendations, such as a proposed schedule for implementation, should be provided where applicable. The management official should be at a level where budgetary decisions can be made and system changes approved.

7.2 The list of recommendations should note which recommendations are required to comply with the minimum security requirements and should be signed by the person responsible for conducting the risk analysis. The completed, documented risk analysis is then forwarded to the appropriate management official for a decision to implement individual recommendations or to accept the risk. The management official documents the decisions by checking the applicable column of Work Form 10, signing Work Form 10, and adding comments where appropriate.

STEP 7 LIST OF RECOMMENDATIONS FOR MANAGEMENT ACTION			
THE FOLLOWING SECURITY MEASURES ARE RECOMMENDED TO ENHANCE SYSTEM SECURITY	MGT DECISION IMPLEMENT	 ACCEPT RISK	RECOMMENDATIONS SUBMITTED BY: Signature/Title Date RECOMMENDATIONS APPROVED / DISAPPROVED BY: Signature/Title Date COMMENTS ON RECOMMENDATIONS BY APPROVING / DISAPPROVING OFFICIAL

WORKFORM 10
RECOMMENDATIONS FOR MANAGEMENT DECISION/ACTION

NIST-114A
(REV. 3-90)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

BIBLIOGRAPHIC DATA SHEET

1. PUBLICATION OR REPORT NUMBER
NISTIR 4387

2. PERFORMING ORGANIZATION REPORT NUMBER

3. PUBLICATION DATE
AUGUST 1990

4. TITLE AND SUBTITLE
U.S. Department of Justice Simplified Risk Analysis Guidelines (SRAG)

5. AUTHOR(S)
Edward Roback, NIST Coordinator

6. PERFORMING ORGANIZATION (IF JOINT OR OTHER THAN NIST, SEE INSTRUCTIONS)
U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
GAITHERSBURG, MD 20899

7. CONTRACT/GRANT NUMBER

8. TYPE OF REPORT AND PERIOD COVERED
NISTIR

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (STREET, CITY, STATE, ZIP)
Reprinted by permission of the U.S. Department of Justice, Justice Management Division, Security and Emergency Planning Staff, ADP/Telecommunications Group, Washington, DC 20530

10. SUPPLEMENTARY NOTES

11. ABSTRACT (A 200-WORD OR LESS FACTUAL SUMMARY OF MOST SIGNIFICANT INFORMATION. IF DOCUMENT INCLUDES A SIGNIFICANT BIBLIOGRAPHY OR LITERATURE SURVEY, MENTION IT HERE.)

The Simplified Risk Analysis Guidelines (SRAG) approach to risk analysis divides systems into three categories: Personal Computers; mainframes, minicomputers, and other remotely accessed automated information systems; and application systems. Each of these categories is further divided depending on whether nonsensitive, sensitive, or classified information is processed, or whether an application is sensitive. The SRAG approach includes seven steps that are required to conduct the risk analysis and to document the results. The last portion of the SRAG is the Appendix, which includes detailed information required to conduct a risk analysis, and a number of tables and work forms for use in conducting and documenting the risk analysis.

12. KEY WORDS (6 TO 12 ENTRIES; ALPHABETICAL ORDER; CAPITALIZE ONLY PROPER NAMES; AND SEPARATE KEY WORDS BY SEMICOLONS)
ADP security, automated information systems security, computer security, risk assessment, risk analysis, risk management.

13. AVAILABILITY

[X] UNLIMITED

[ ] FOR OFFICIAL DISTRIBUTION. DO NOT RELEASE TO NATIONAL TECHNICAL INFORMATION SERVICE (NTIS).

[ ] ORDER FROM SUPERINTENDENT OF DOCUMENTS, U.S. GOVERNMENT PRINTING OFFICE, WASHINGTON, DC 20402.

[X] ORDER FROM NATIONAL TECHNICAL INFORMATION SERVICE (NTIS), SPRINGFIELD, VA 22161.

14. NUMBER OF PRINTED PAGES
60

15. PRICE
A04

ELECTRONIC FORM